Pak. J. Engg. & Appl. Sci. Vol. 13, July, 2013 (*p.* 94-100)

A Mitigation Approach to Counter Initial Ranging Based DoS Attacks on IEEE 802.16-2009

Yasir Saleem[1], Sheraz Naseer[1,2], Khadim H. Asif[1], Touqir Ahmad[1], Khawar Bashir[1,3], Muhammad Younus Javed[2] and Ayesha Altaf[2]

1. Department of Computer Science & Engineering, University of Engineering & Technology, Lahore
2. National University of Sciences and Technology, Islamabad
3. University of Veterinary and Animal Science, Lahore

Abstract

In recent years increase in wireless accessed devices does not prerequisite any evidence. Security is the main concern for the researchers in 802.16e now-a-days. The layer structures defines that the security sub-layer resides over the physical layer and provides security on the link layer.This paper discusses the security threats present and still unsolved at the initial network entry stage. A mitigation approach to counter Initial Ranging Based DoS attacks on IEEE 802.16-2009 are particularized in this paper. Furthermore the existing solutions of initial ranging vulnerability are analyzed and their limitations are discussed. Proposed solution was checked against these limitations to ensure their absence. Moreover the solution was implemented in OMNET++ and results were analyzed to ensure the practicality and efficiency.

1. Introduction

IEEE 802.16-2009 [1] is the rollup of 802.16-2004, 802.16-2004/Cor 1, 802.16e, 802.16f, 802.16g and P802.16i) for providing enhanced performance and security of Wireless MAN. Security is the main concern for the researchers in 802.16e now-a-days. Security sub-layer resides over the physical layer and provides security on the link layer. Security sub-layer in Media Access Control (MAC) layer in 802.16e [2] is used to deal with privacy, authentication and key exchange issues.

One of the most severe and still un-resolved threats is based on initial network entry. Denial of service attack(DoS) routine can be used to disturb the quality parameters in IEEE 802.16-2009.DoS is considered in detail by authors in literature [3-5].

Literature review has revealed that very little research work has been published to secure initial-ranging of SS and initial ranging messages are un-authenticated, un-encrypted and stateless. These vulnerabilities and weaknesses exposing security threat presented in above mentioned networks to DoS attacks can also be found in literature particularly in [6-8]. The complete network entry procedure between BS and SS/MS is unprotected. Adversaries can not only listen to the traffic, they can also use this information to forge different kinds of frames to wreak havoc on the network. Worst part is that, these messages does not come under the security sub-layer umbrella of IEEE 802.16 and are completely on the mercy of attacker.

A mechanism is proposed to generate a shared secret at the first opportunity in network ranging and then use this secret to secure the initial ranging communication depending upon the security needs of 802.16 based networks under consideration. The solution proposed can mitigate attacks based on initial entry including RNG-REQ, RNG-RSP, DBPC-REQ/RSP and SBC-REQ/RSP.

This mechanism is also implemented in simulated environment between BS and SS and packets are sent and received. The rejection pattern and results have ensured the practicality and efficiency of proposed scheme.

2. Background

2.1 Attacks based on initial Network Entry

i. An adversary can create a fakeRNG-RSP message to alter the power level of SS to minimum level forcing it to barely transmit for BS triggering initial ranging procedure repeatedly [7].

ii. Attackers can also mount water torture DoS attacks by changing power level to maximum causing drastic reduction in battery life.

iii. Attacker can change the SSs Downlink channel to an altered frequency range. This attack has multiple threat vectors. If the attacker has rouge BS operating in that altered frequency range it can do multiple types of malafide actions to SS and deny service from legitimate BS. In absence of rouge BS, the victim still has to scan and find its way back to appropriate channel. Depending upon frequency range, it will take some time to find frequency of legitimate BS during which SS is unable to use legitimate service [7].

iv. Alternatively an attacker can alter only uplink channel to disrupt the communication between SS and BS.

2.2 Existing Mitigation approaches and limitation

In this section, existing schemes to protect initial network entry of SS in IEEE 802.16 based networks are discussed along with their limitations. These schemes are proposed by [3], [4] and [5].

Scheme proposed by T. Shon et al. [3]

2.2.1 Mechanism

In this section, existing schemes to protect initial network entry of SS in IEEE 802.16 based networks are discussed along with their limitations. These schemes are proposed by [3], [4] and [5].

Scheme proposed by T. Shon et al. [3]

2.2.2 Mechanism

According to them, "the Initial ranging vulnerability of 802.16-2009 can be overcome by using Diffie-Hellman key agreement protocolat initial network entry. Initial ranging processbegins when SS receives UL-MAP control message including initial ranging region. SS chooses a random ranging code and sends the selected code to BS. BS, on reception of UL-MAP, notifies SS regarding the acceptance of ranging code with RNG-RSP message. From the proposed security approach in initial network entry, a selected ranging code is not only used for Mobile WiMAX communication, but also for generating a prime number 'p' as one of global variables for applying Diffie-Hellman key agreement to initial network entry process. Similarly, SS generates the other global variable 'q' and public/private key pair, and then sends them to BS. BS,on reception ofSS public key and global variables (prime number and its primitive root) performs verification. If the received key and variables are verified, BS sends its public key to SS. Thus, BS and SS can mutually share DH global variables and public key of each other during initial ranging process. Of these parameters, they can generate a shared common key called "pre-TEK" independently and establish secret communication channels" [3].

2.2.3 Limitations

The proposed scheme suffers from following short comings.

i) It does not provide any mechanism to generate a prime 'P' from ranging code which is essentially an 8 bit number.

ii) It is not obvious whether the SS or the BS will generate the Prime 'P'.

iii) The proposed scheme places the bar of generating a random Primitive root 'g' of a random prime 'P' on SS. Such calculation may involve either tremendous amount of processing time or storage space if such values are pre-computed. SS essentially is a resource limited entity and placing such a bar on SS itself causes a Denial of Service and wastes the precious resources of SS. This problem becomes more aggravated in case of MSs.

iv) As no concrete mechanism is provided to generate P or g, it is unclear how such a value will be verified by BS.

Scheme proposed by S. Maru et al. [4]

2.2.4 Mechanism

S Maru et al. [**4**] devise**"***t**ransmitting the initial ranging messages in secure manner by using public key cryptography. Performing encryption of the messages will make it difficult for the attacker to identify which messages are being transferred at a particular instant hence making theeffortto disrupttrafficexponentially difficult*."[4].

2.2.5 Limitations

i) Although the built-in digital certificates may be used to securely transmit initial ranging but this require fundamental change in protocol because the digital certificates are exchanged after initial

ranging and before that the communicating parties have no knowledge of certificates.

ii) If somehow certificates are known at initial ranging time, the messages can be secured by either encryption or attaching MAC. Bothe these scenarios are not efficient in wireless environment.

a) Encryption/Decryption is less efficient because public key cryptography using RSA is inherently very slow due to involvement of large Primes and encrypting/decrypting time critical management messages using public key crypto is not efficient.

b) To generate MAC, both parties must have a shared key, which is not the case in PKC. Although a shared key may be prepared using PKC, such preparation will require a separate mechanism.

Scheme proposed by A Altaf et al. [5]

2.2.6 Mechanism

The visual cryptography scheme presented in [5] may be extended for initial network entry vulnerability. But such an extension will suffer from limitations.

2.2.7 Limitations

i) As the scheme proposed by [5] mandates the use of subject field of digital certificate, its extension to initial network entry would require the presence of digital certificates from communicating parties which in turn would require fundamental change in how the existing protocol works.

ii) Furthermore, the proposed scheme requires trusted third party (TTP) server for the implementation, it may not be suitable when considering the end to end network architecture.

3. Proposed Solution

3.1 Mechanism

The scheme requires that a public Prime number 'P' is known to both BS and SS during initial ranging time. In our proposed method, BS shall maintain a list of 'n' number of primes along with their primitive roots, where n <= 255 and map all possible 8 bit values to n. For example consider the scenario where BS has maintained a list of 15 primes and an SS has chosen 134 as CDMA code. BS may allocate the prime at index n where n= 134 mod 15 i.e. n=14 mod 15, hence BS will use prime at index 14 to generate shared secret with SS. As prime 'P' is public parameter, BS may maintain a random list of 'P' to use in communications. After allocation of Basic Connection ID (BCID), BS and SS will have the knowledge of BCID and initial ranging CDMA codes as chosen randomly by MS/SS. BCID is allocated by base station from designated pool to entering subscriber (SS).

Both parties can separately calculate a number 'n'. To avoid unnecessary changes in existing standard, a slightly extended version of dot16kdf algorithm is devised as shown in figure.

The Dot16KDF algorithm is a CTR (Counter) mode structure that can be used to derive an arbitrary amount of keying material from source keying material [2].

After calculation, SS will request the BS to check 'n' for primitive root property. BS will perform check to verify whether the calculated number 'n' is primitive root 'g' of finite field of P, denoted by GF(P) or not. If the number is primitive root BS will respond with empty RNG-RSP message otherwise it will send the difference between 'n' and nearest 'g' value greater than n.

It is to be noted that the number of prime roots for any given P is given by following formula:

Number of Primitive Roots of P = Ø (Ø (P))

where Ø denotes Euler's totient function. This means that for any given Prime 'P' and number 'n' A prime root will be available at most within the range $(n + 2^6)$.

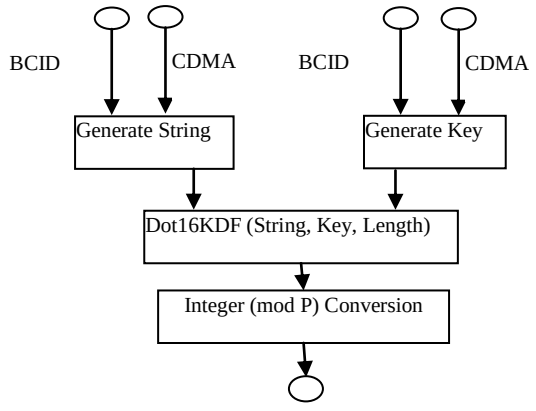

Fig. 1 Extended dot16KDF Algorithm

SS, on receiving the difference, will adjust the value of Prime-root g such that:

$$= n + difference \quad (1)$$

Once both parties possess 'g' Diffie-Hellman key agreement scheme can be used as follows:

SS will select a random number 'X_{ss}' in the range 0 to P-1, where P denotes the prime and calculate 'Y_{ss}' such that:

$$Y_{ss} = g^{Xss} \bmod P \quad (2)$$

SS will send 'Y_{ss}' to BS. Hence 'X_{ss}' will serve as the private key of the SS and 'Y_{ss}' will serve as the public key of the BS. Similarly BS will select a random number 'X_{BS}' in the range 0 to P-1, where P denotes the prime and calculate 'Y_{BS}' such that:

$$Y_{BS} = g^{XBS} \bmod P \quad (3)$$

BS will send 'Y_{BS}' to SS. Hence 'X_{BS}' will serve as the private key of the SS and 'Y_{BS}' will serve as the public key of the BS. It needs to be noted that the generator 'g' will be different for each SS and BS's public private key pair will be different for each SS.

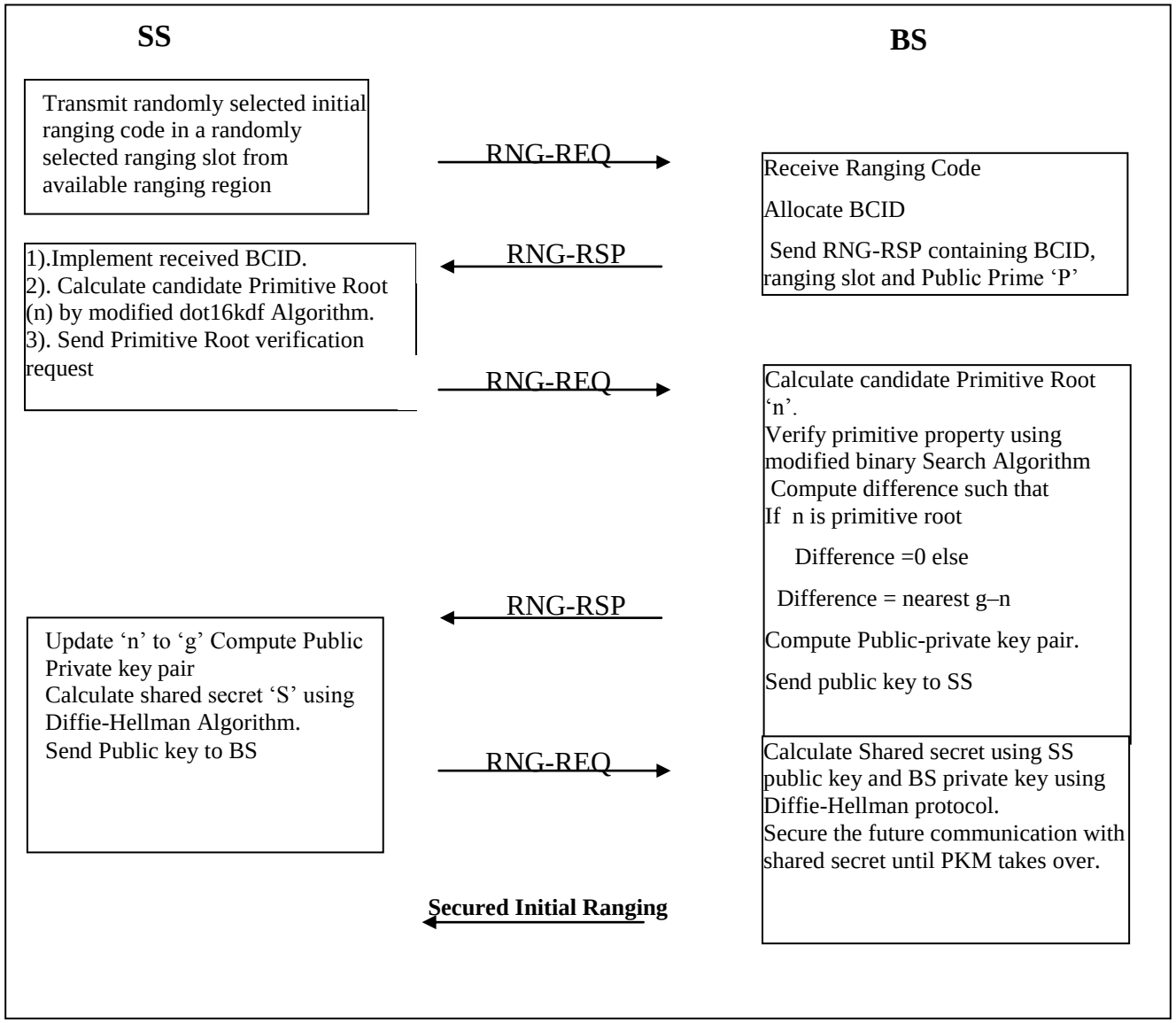

Fig. 2 Algorithm for proposed approach

On receiving respective public Keys both SS and BS will calculate the session key such that:

$$\textbf{Shared Key}_{SS} = Y_{BS}^{Xss} \bmod P \quad (4)$$

$$\textbf{Shared Key}_{BS} = Y_{SS}^{XBS} \bmod P \quad (5)$$

Using these session keys, further network entry is secured either by applying CBC/Hash MAC or by encrypting the initial ranging messages depending upon the level confidentiality required.

4. Comparison with Existing Schemes

This section provides a comparison between existing schemes, and proposed solution. This section further elaborates the proposed solution to describe how it overcome the limitations of existing schemes.

4.1 Comparison with [3]

i) Our proposed method provides echanism to calculate Prime 'P'. BS shall maintain a list of 'n' number of primes along with their primitive roots, where n <=255 and map all possible 8 bit values to 'n'.

ii) Our proposed Scheme, in contrast to [3] places the bar of generating a random Primitive root 'g' of a random prime 'P' on BS. In our proposed scheme, both SS and BS separately compute a candidate primitive-root by using extended dot16KDF algorithm while the onus of verification of the primitive root is on BS which is not a resource constrained entity.

4.2 Comparison with [4]

Maru et al. [4] devise transmitting the initial ranging messages securely by built-in digital certificates using public key cryptography. This requires fundamental change in protocol because in all revisions of 802.16 standards, the digital certificates are exchanged after initial ranging. We do not propose the use of public key cryptography to secure the initial ranging.

4.3 Comparison with [5]

The visual cryptography scheme presented in [5] may be extended for initial network entry vulnerability. As the scheme proposed by [5] mandates the use of subject field of digital certificate, its extension to initial network entry would require the presence of digital certificates from communicating parties which in turn would require fundamental change in how the existing protocol works because digital certificates are not known at initial ranging time and are communicated once initial ranging is complete.

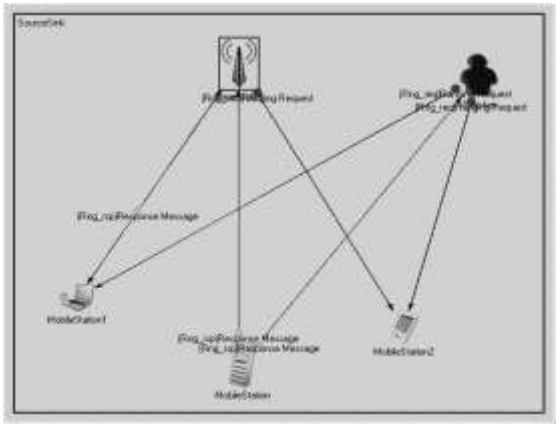

Fig. 3 Network for simulation

Our proposed solution does not mandate the use of digital certificates.

4.4 Implementation and Analysis

This section provides the implementation of proposed solution using the OMNET++ simulator. The Network architecture is shown in figure 3. The architecture consists of an Attacker with 3 Mobile Stations and one Base Station. The small numeric number and bars representing the values and also colors in real simulated results respectively. The figure is showing malicious packets and rest can be understood by the Table 2 in view of Figure 5.

Following scenarios have been implemented using the abovementioned Network Architecture.

i) The first scenario of simulation consists of Network conditions without proposed solution.

ii) In second scenario of simulation, we have implemented our proposed solution in existing Network described in figure 3.

Using our devised algorithm, each BS-SS pair develops a unique shared secret key depending upon the chosen CDMA codes and BCID. Once the shared key is in place,results of scenario ii shows the unsuccessful attempts to launch RNG-RSP DoS attack as shown in figure.

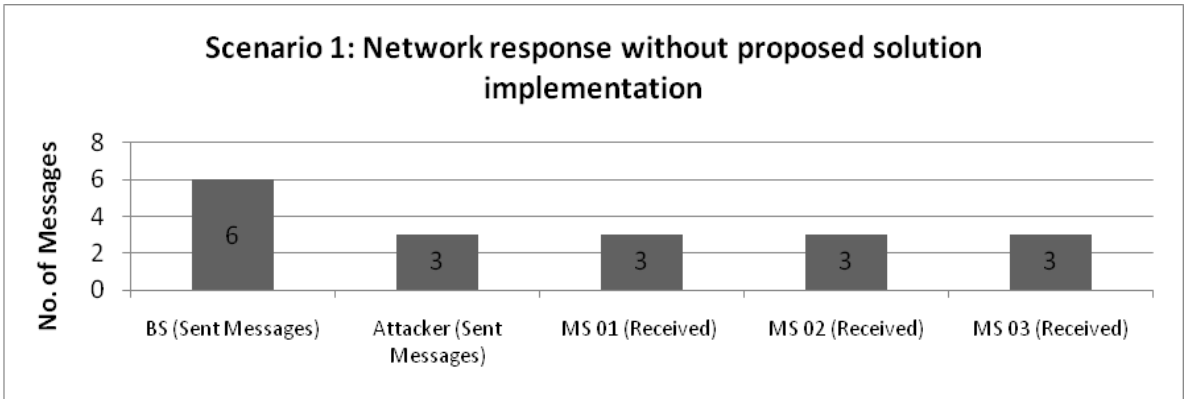

Fig.4 Bar chart displaying RNG-RSP attack on Network

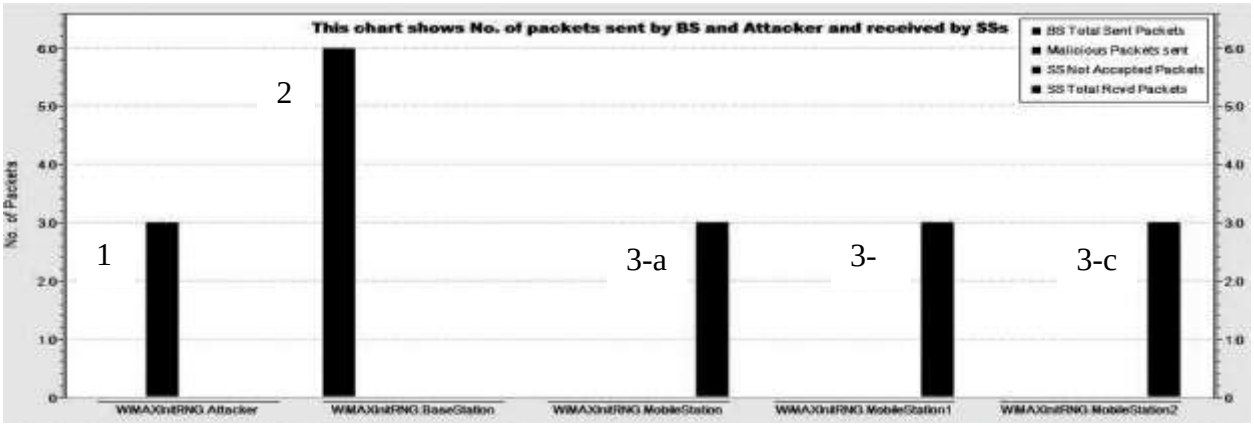

Fig.5 Bar chart displaying RNG-RSP attack on Network

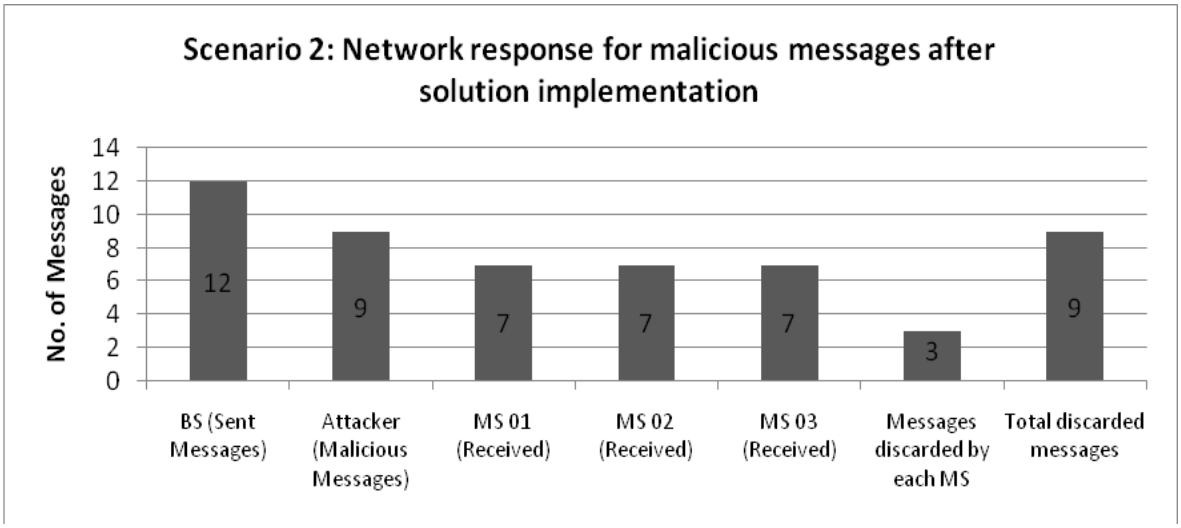

Fig. 6 Bar chart displaying impact of proposed solution on Network

Table 2 Analysis messages during scenario presented in Figures 3 and 4.

Event Description	Without Proposed Solution	With Proposed Solution
Messages sent by BS	6	12
Messages sent by Attacker	3	9
Messages received by individual SSs	3	7
Messages discarded by each SS	0	3
Total no. of discarded messages	0	9

Results of scenario I, as shown in Fig 4, depicts that the Attacker sent 3 forged messages displayed in Figure 3 and all the messages were accepted as legitimate by all 3 SSs. This clearly shows that in addition to 2 messages sent by BS all 3 SSs have accepted a message from the Attacker. This is because the SS has no way to identify whether the RNG-RSP message is a legitimate one or illegitimate.

In second scenario we have implemented our proposed solution. The simulation results are shown in bar graph representation for easy and smooth view of reader. Results shown in figure5 depicts the network situation after having a RNG-RSP attack while proposed solution is in place. It is evident from figure 5 that total No of messages sent by attacker is equal to total No. of messages discarded by SSs. Furthermore No. of Illegal Messages received by individual SS is the same as no. of Messages discarded. This analysis provides us reasonable confidence regarding the proposed solution.

5. Conclusions

The implementation and analysis discussed in section 5 are done using simulated environment. The two scenarios are implemented, one without our proposed scheme as shown in figure 4 and second with our proposed scheme in figure 5. The analysis of results shown in Table 1 has proved that Although IEEE 802.16e has a strong and promising security Architecture, there are still some gaps which need to be addressed.

In this paper, a mitigation approach is proposed to counter initial ranging based DoS attacks on IEEE 802.16-2009. Moreover, the proposed solution was implemented and analyzed to confirm its viability.

6. References

[1] IEEE Std. 802.16-2009, "IEEE Standard for Local and Metropolitan Area Networks, part 16: Air Interface for Broadband Wireless Access Systems", IEEE Press, May 2009.

[2] National Institute of Standards and Technology Special Publication 800-127 (Draft) Natl. Inst. Stand. Technol. Spec. Publ. 800-127, 46 pages (Sep. 2009)

[3] Taeshik Shon, Wook Choi: An Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions, First International Conference, NBiS 2007, LNCS, Vol. 4650, pp. 88-97, 2007.

[4] Maru,S. Brown, T.X. "Denial of Service Vulnerabilities In the 802.16 Protocol" DOI: 10.4108/ICST.WICON2008.4849 http://dx.doi.org/10.4108/ICST.WICON2008.4849

[5] A.Altaf, R.Sirhindi and A.Ahmed, "A Novel Approach against DoS Attacks in WiMAX Authentication using Visual Cryptography", Proc. of 2nd Int'l Conf. on Security Info. Syst. and Tech., 2008, pp. 238–242

[6] SherazNaseer, Dr. Muhammad Younus, Attiq Ahmed, "Vulnerabilities Exposing IEEE 802.16e Networks To DoS Attacks: A Survey", in International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2008.

[7] Boom D., Buddenberg R., Denial of Service Vulnerabilities in IEEE 802.16 Wireless Networks IEEE C802.16e-04/406.

[8] M. Shojaei, N. Movahhedinia, and B. Tork Ladani, "An Entropy Based Approach for DDoS Attack Detection in IEEE 802.16 Based Networks," in Advances in Information and Computer Security. vol. 7038, T. Iwata and M. Nishigaki, Eds., ed: Springer Berlin Heidelberg, 2011, pp. 129-143.